⑲日本国特許庁（JP）　⑪特許出願公開

⑫公開特許公報（A）　昭61－107375

⑤Int.Cl.⁴　識別記号　庁内整理番号　⑬公開　昭和61年(1986)5月26日
G 09 C　1/00　7368－5B

審査請求　未請求　発明の数 1　（全4頁）

⑤④発明の名称　暗号装置のランダム転置テーブル作成方法

⑳特　願　昭59－229322
㉒出　願　昭59(1984)10月31日

⑦②発明者　東　充宏　川崎市中原区上小田中1015番地　富士通株式会社内
⑦②発明者　鳥居　直哉　川崎市中原区上小田中1015番地　富士通株式会社内
⑦②発明者　秋山　良太　川崎市中原区上小田中1015番地　富士通株式会社内
⑦①出願人　富士通株式会社　川崎市中原区上小田中1015番地
⑦④代理人　弁理士　松岡　宏四郎

明　細　書

1．発明の名称

暗号装置のランダム転置テーブル作成方法

2．特許請求の範囲

ブロック転置テーブルとエレメント転置テーブルから構成されるランダム転置テーブルを使用して平文データをランダム転置して暗号化する暗号装置に於いて、整数nと整数mを夫々任意に設定し、ブロック暗号器から出力される乱数列を使用し、前記乱数列の頭から該整数nより大きい数を除外して該整数n個取り出して該ブロック転置テーブルとし、引続き前記乱数列から該整数mより大きい数を除外して該整数m個取り出して第1の該エレメント転置テーブルとし、以下同様に前記乱数列から該整数mより大きい数を除外して該整数m個取り出して第nの該エレメント転置テーブルとすることを特徴とする暗号装置のランダム転置テーブル作成方法。

3．発明の詳細な説明

〔産業上の利用分野〕

本発明は暗号装置に係り、特にランダム転置テーブルを使用する暗号装置に関するものである。

〔従来の技術〕

暗号装置には従来から種々の方式があるが、其の一つにランダム転置テーブルを使用する暗号装置がある。

此処で云うランダム転置とは送信しようとする平文データ（普通の文章）を複数個のブロックに分け、其のブロックの位置を置き換えて原データとは思えないようにする処理を云う。

第2図は従来の暗号装置の一構成例を示す。

図中、1は暗号装置、2はブロック暗号器、3はランダム転置装置、4はランダム転置テーブル、4aはブロック転置テーブル、4bはエレメント転置テーブルである。尚以下全図を通じ同一記号は同一対象物を表す。

従来の暗号装置1は図示する様にランダムデータを発生するブロック暗号器2と暗号処理を行うランダム転置装置3から構成されている。

第3図はブロック暗号器の構成の一例を示す図

である。

ブロック暗号器2はランダムなデータ列をブロック単位で発生する一種の乱数表発生装置で、或るブロック長のキーデータを外部から入力するとブロック暗号器2の中で同じブロック長の乱数列を発生する。此の発生した乱数列を入力して順次次の乱数列を発生させる。

第4図はランダム転置装置の構成の一例を示す図である。

「ランダム転置装置3はブロック暗号器2より発生した乱数列からブロック転置テーブル4aとエレメント転置テーブル4bを作成する。

此の両転置テーブルにより入力データブロックに対し先づブロック転置処理を行い、次に各ブロックに対しエレメント転置を行って暗号文として出力する。」

此の様に平文データをランダム転置するために使用する転置テーブルには解読を防ぐために以下に述べる性質が必要であるといわれている。

イ）転置テーブル内には同じ値が2つ以上あってはならない。

ロ）転置テーブル内にはテーブル容量より大きい値があってはならない。

ハ）転置されないデータがあってはいけない。

然しブロック暗号器から発生するランダムデータ列より上記の性質を満たし、且つランダム性を失わない様なランダム転置テーブルを作成するにはガットアンドトライ方式に依る為其の都度任意に作成するうまい方法は従来存在しなかった。

〔発明が解決しようとする問題点〕

本発明の目的はブロック暗号器から発生するランダムデータから或る一定の性質を持つ任意の大きさのランダム転置テーブルを比較的速く作成出来る方法を提供することである。

〔問題点を解決するための手段〕

問題点を解決するための手段は、ブロック転置テーブルとエレメント転置テーブルから構成されるランダム転置テーブルを使用して平文データをランダム転置して暗号化する暗号装置に於いて、整数nと整数mを夫々任意に設定し、ブロック暗号器から出力される乱数列を使用し、前記乱数列の頭から該整数nより大きい数を除外して該整数n個取り出して該ブロック転置テーブルとし、引続き前記乱数列から該整数mより大きい数を除外して該整数m個取り出して第1の該エレメント転置テーブルとし、以下同様に前記乱数列から該整数mより大きい数を除外して該整数m個取り出して第nの該エレメント転置テーブルとすることにより達成される。

〔作用〕

本発明に依ると転置処理で利用されるランダム転置テーブルをブロック転置部分とエレメント転置部分に分け、ブロック暗号器から発生するランダムデータから上記説明の如く効率良くランダム転置テーブルを作成するようにする為ランダム転置テーブルの作成が直線的に比較的速く作成出来ると云う効果が生まれる。

〔実施例〕

第1図は本発明に依るランダム転置テーブルの作成方法を示す図である。

以下図に従って本発明の詳細を説明する。

本発明ではブロック暗号器2から出力された乱数列を下記の条件を満たす様に順次並べて行く。

本例では一例として16進コードを使用しているので乱数表で取り扱う数字は1～9、A、B、C、D、E、Fの16種類とする。

1）ブロック転置テーブル作成時には1～n以外の数、エレメント転置テーブル作成時には1～m以外の数は無視する。

2）1つのテーブル内には同じデータが2つ以上あってはならない。

3）転置されない領域があってはならない。

但し、m、nは共に正の整数である。

例えば第1図(a)に示す様な乱数列がブロック暗号器2から発生したとする。

尚此処では簡単のためn＝3、m＝4、即ち、n×m＝12　の場合を例にとって本発明に依るランダム転置テーブルの作成に就いて述べる。

最初の乱数は＂3＂であるので、ブロック転置テーブル4aの先頭に＂3＂を入れる。

2番目は"F"であるので無視する。

3番目は"1"であるので、ブロック転置テーブル4aの2番目に"1"を入れる。

4番目は"2"であるので、ブロック転置テーブル4aの3番目に"2"を入れる。

n=3 であるので、此れでブロック転置テーブル4aは出来上がる。

続いて乱数列の5番目は"2"であるので、第1エレメント転置テーブル4bの1番目に"2"を入れる。

次に乱数列の6番目は"A"、7番目は"7"、8番目は"6"であるので共に無視する。

乱数列の9番目は"1"であるので、第1エレメント転置テーブル4bの2番目に"1"を入れる。

乱数列の10番目は"4"であるので、第1エレメント転置テーブル4bの3番目に"4"を入れる。

乱数列の11番目は"A"であるので無視し、乱数列の12番目は"3"であるので、第1エレメント転置テーブル4bの4番目に"3"を入れる。

以下同様にして第2、第3のエレメント転置テーブル4bの作成を行う。

第1図(b)は此の様にして作成されたブロック転置テーブル4a、エレメント転置テーブル4bを示す。

此等の転置テーブルを使用して第1図(c)に示す様に実際の転置を行う。

第1図(c)のAは平文データを示し、12字で構成されている。1～4は第1ブロック、5～8は第2ブロック、9～12は第3ブロックである。

ブロック転置テーブルの内容は"3.1.2"であるので、1→3、2→1、3→2というようにブロック転置を行う。此の結果第1図(c)のBに示す様にブロック転置される。

次にエレメント転置テーブルの1番目の内容は"2.1.4.3"であるので、第1ブロック中のエレメントを1→2、2→1、3→4、4→3というようにエレメント転置を行う。

即ち、Bの第1ブロックは5.6.7.8であるので、エレメント転置テーブルの1番目の内容は"2.1.4.3"に従い、5は2番目へ、6は1番目へ、7は4番目へ、8は3番目に移すので、6.5.8.7となる。

同様にエレメント転置テーブルの2番目の内容は"4.1.2.3"であるので、第2ブロック中のエレメントを1→4、4→1、3→2、2→3というようにエレメント転置を行う。

同様に第3ブロック中のエレメントについてエレメント転置を行う。

此の様にしてエレメント転置を行った結果得られたデータは第1図(c)のCに示す様なデータとなり、此れを暗号文として送出する。

受信側では以上の操作と全く逆の処理を行ってデータを復号する。

上記説明の様なランダム転置テーブル作成方法によれば、ブロック暗号器2から得られる乱数列より前述の条件を満たすランダム転置テーブルが高能率で得られる。

〔発明の効果〕

以上詳細に説明した様に本発明によれば、ブロック暗号器から得られる乱数列を有効的にテーブル情報として活かすことが出来、任意の大きさのランダム転置テーブルを比較的高速度で作成出来ると云う大きい効果がある。

4．図面の簡単な説明

第1図は本発明に依るランダム転置テーブルの作成方法を示す図である。

第2図は従来の暗号装置の一構成例を示す。

第3図はブロック暗号器の構成の一例を示す図である。

第4図はランダム転置装置の構成の一例を示す図である。

図中、1は暗号装置、2はブロック暗号器、3はランダム転置装置、4はランダム転置テーブル、4aはブロック転置テーブル、4bはエレメント転置テーブルである。

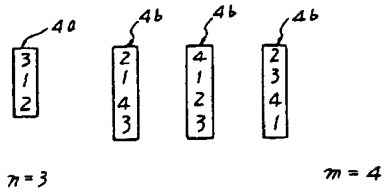
代理人　弁理士　松岡宏四郎

第 1 図

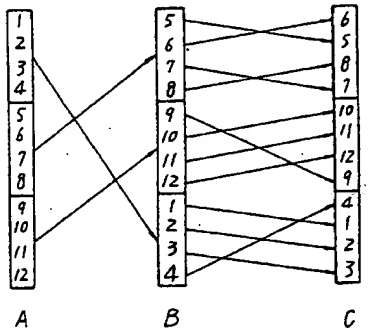
(a) 3F 12 2A 76 14 A3 EC 4A 12 3C 123

44 1AF ---------

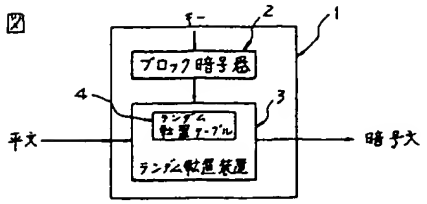
(b)



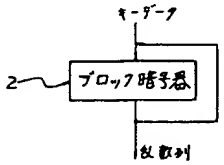
(C)



第 2 図



第 3 図



第 4 図